ABSTRACT OF THE DISCLOSURE

HIERARCHICAL CORRELATION OF INTRUSION DETECTION EVENTS

A method, computer program product, and apparatus for presenting data about security-related events that puts the data into a concise form is disclosed. Events are abstracted into a set data-type. Sets with common elements are grouped together, and summaries of the groups—"situations" are established from groups whose severity exceeds a threshold value. These groups and situations are then propagated up a hierarchical arrangement of systems and further aggregated so as to provide summary information over a larger group of systems. This hierarchical scheme allows for scalability of the event correlation process across larger networks of systems.